CHECKLIST DE SÉCURITÉ

10 conseils pour protéger votre entreprise des risques internes

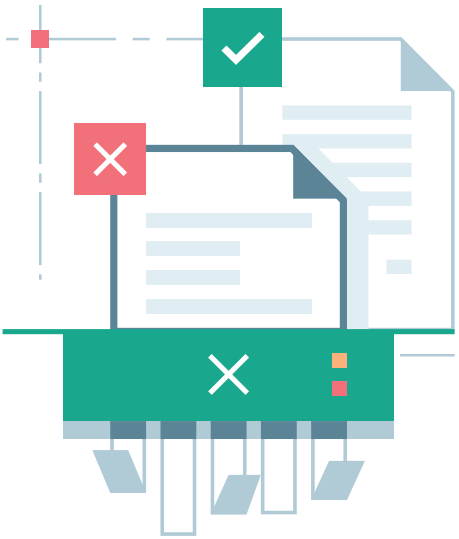
87 800 $ Impact financier total moyen d'une violation de données pour les petites et moyennes entreprises[1].

992 000 $ Impact financier total moyen d'une violation de données pour les entreprises[2].

46 % Événements de sécurité auxquels des salariés négligents ou mal informés ont contribué[3].

35 % Entreprises qui tenteront de réduire les failles de sécurité en proposant des formations supplémentaires à leur personnel[4].

61 % Cadres supérieurs occupant une fonction non informatique qui affirment que la protection des données est un problème de sécurité informatique majeur[5].

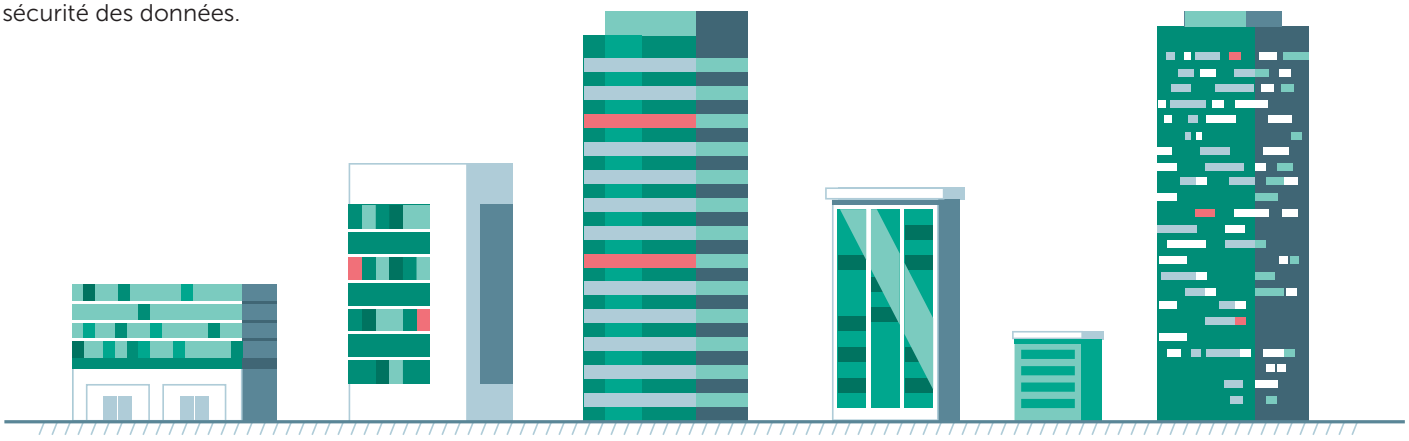


1-5. *Enquête 2017 sur les risques de sécurité informatique au niveau mondial* par Kaspersky Lab et B2B International

La menace se trouve à l'intérieur de votre entreprise

Regardez au sein de votre entreprise et vous trouverez l'une des plus grandes menaces de sécurité informatique auxquelles vous êtes confronté : vos collègues. Même les salariés les mieux intentionnés, les plus grands défenseurs de votre entreprise, risquent de divulguer des données sensibles ou d'introduire par inadvertance des programmes malveillants qui peuvent faire des ravages sur votre réseau et vos systèmes.

Pour les entreprises de toutes tailles, les menaces en provenance de l'intérieur constituent une préoccupation constante, parmi les plus difficiles à prévoir. Avec des salariés qui utilisent plusieurs appareils, souvent sur plusieurs sites, votre département informatique doit relever un défi de taille : surveiller un périmètre qui est une cible mouvante. Toutefois, certaines mesures peuvent assurer votre protection. En étudiant attentivement la question de la sécurité informatique sous tous les angles, vous pouvez atteindre cet équilibre important entre permettre aux salariés d'accéder aux informations dont ils ont besoin et assurer la sécurité des données.



Dix conseils de sécurité pour protéger votre entreprise des risques internes

1. Vos salariés sont votre première ligne de défense.

À RETENIR :
Dans toute organisation, plus les salariés en savent sur la façon de protéger l'entreprise, mieux l'entreprise est protégée. Assurez-vous que tous les salariés connaissent et respectent les politiques de sécurité de l'entreprise. Publiez les politiques clairement et répondez aux questions qu'ils se posent régulièrement.

2. La formation des salariés est un investissement justifié.

À RETENIR :
80 % des cyberincidents ont pour origine une erreur humaine. Réduire ce pourcentage commence par sensibiliser les salariés aux dangers des attaques qui les visent spécifiquement via le piratage informatique. Le phishing, les ransomwares, et le phishing ciblé sont des moyens par lesquels les cybercriminels accèdent à votre organisation par l'intermédiaire des salariés. Les propres données de Kaspersky Lab montrent que les entreprises qui forment leurs salariés à la cybersécurité parviennent à leur faire appliquer leurs nouvelles connaissances avec un taux de réussite de 93 %. La formation est incontournable, surtout lorsque vous utilisez des méthodes variées et créatives. Les séances en face à face, jumelées avec des webinaires, des infographies et des vidéos sont des méthodes qui contribuent à diffuser le message.

3. La formation des salariés commence par les dirigeants de votre entreprise.

À RETENIR :
La plupart des cadres comprennent que la cybersécurité est un problème, mais beaucoup ne réalisent pas l'importance du rôle qu'ils ont à jouer. En promouvant une culture de sensibilisation à la cybersécurité aux échelons hiérarchiques supérieurs de votre organisation, les cadres peuvent non seulement contribuer à ce que les salariés prennent la question au sérieux, mais également à ce que votre organisation soit mieux protégée. En outre, de nombreux conseils d'administration savent désormais qu'ils peuvent, dans de nombreux cas, être tenus pour légalement responsables en cas de violation de données et qu'ils devront démontrer qu'ils ont fait preuve de diligence raisonnable pour protéger leurs clients et leurs actifs. Lorsque vous abordez ce sujet avec les cadres, il est important de ne pas présumer qu'ils comprennent tous les enjeux liés à la sécurité informatique. En comblant leurs lacunes, vous les aiderez à saisir la complexité de cette question et à promouvoir la sensibilisation au sein de votre organisation.

4. Tous les salariés doivent savoir comment informer le département informatique de tout incident de sécurité.

À RETENIR :
Expliquez-leur les signes d'une violation de données et indiquez-leur qui appeler dans ce cas. Les numéros et les contacts doivent être clairement communiqués. Nombre de salariés peuvent hésiter à tirer la sonnette d'alarme, mais leur vigilance est une protection vitale. Ils doivent faire preuve de prudence et solliciter immédiatement le département informatique en cas de soupçon.

5. Gardez le contrôle sur les droits d'accès et les privilèges des utilisateurs.

À RETENIR :
L'une des mesures les plus importantes de votre service informatique est de garder le contrôle sur les utilisateurs qui ont accès à certains programmes, appareils et données sensibles au sein de l'entreprise. Cela implique de comprendre les nombreux rôles différents et, potentiellement, de limiter l'accès à certains salariés pour garantir un niveau de protection supérieur.

6. Conservez un registre de tous les droits et privilèges.

À RETENIR :
Lors d'un incident de sécurité, savoir qui a accès à quelle partie de votre organisation peut vous faire gagner beaucoup de temps. L'enregistrement de tous les droits d'accès et privilèges des utilisateurs peut accélérer le travail de votre département informatique et contribuer à atténuer les dégâts plus rapidement.

7. Effectuez des analyses régulières pour détecter les vulnérabilités système et tenir vos services réseau à jour.

À RETENIR :
Vos systèmes et votre réseau évoluent en permanence. L'arrivée de nouveaux salariés et les départs réguliers imposent une vérification fréquente des nouveaux appareils et programmes. En outre, les utilisateurs ont souvent besoin de nouveaux outils dans le cadre de leur travail, ce qui ajoute régulièrement de nouveaux appareils et programmes à votre réseau. Il est important de détecter les vulnérabilités en planifiant des analyses régulières de l'ensemble de votre système.

8. Lorsque vous détectez des services réseau et applications vulnérables, déterminez si la mise en place de nouvelles politiques est nécessaire.

À RETENIR :
Les analyses de votre réseau peuvent révéler des vulnérabilités inattendues. Après avoir effectué une analyse, réévaluer si vous devez ou non mettre à jour vos politiques et procédures afin de rester protégé.

9. Mettez à jour les composants et applications vulnérables.

À RETENIR :
Des correctifs pour les composants et applications vulnérables sont régulièrement mis à disposition par les éditeurs afin de remédier aux vulnérabilités. Il est essentiel d'exécuter ces mises à jour, qui peuvent souvent être effectuées sur une base hebdomadaire régulière.

10. Mettez en place une solution de sécurité multi-niveaux.

À RETENIR :
Il est impossible d'empêcher toute erreur humaine. La mise en œuvre d'une solution multi-niveaux garantit que les menaces sont évaluées sous plusieurs angles. Cette solution doit être une composante essentielle de votre plan de sécurité global.

True Cybersecurity : solutions pour les entreprises

L'approche True Cybersecurity de Kaspersky Lab associe une sécurité multi-niveaux, des renseignements sur les menaces à partir du Cloud et le machine learning pour protéger votre entreprise contre les menaces auxquelles elle est confrontée. Non seulement la solution True Cybersecurity prévient les attaques, mais elle les prédit, les détecte et y répond rapidement, tout en assurant la continuité des activités de votre entreprise.

À propos de Kaspersky Lab

Kaspersky Lab est une des entreprises de cybersécurité du monde connaissant la croissance la plus rapide. C'est aussi la plus importante société privée du secteur. La société est classée parmi les 4 premiers fournisseurs de solutions de sécurité informatique pour utilisateurs de terminaux (IDC, 2014). Depuis 1997, Kaspersky Lab n'a cessé d'innover en matière de cybersécurité. Elle propose des solutions de sécurité numériques efficaces et une surveillance des menaces/Threat Intelligence à destination des grands comptes, des PME/TPE et des particuliers. Le groupe Kaspersky Lab est présent dans près de 200 pays et territoires, offrant une protection à plus de 400 millions d'utilisateurs à travers le monde.

Pour en savoir plus sur la cybersécurité : **www.viruslist.fr**

www.kaspersky.fr
#truecybersecurity

Kaspersky Lab France
Immeuble l'Européen, Bât C, 2 rue Joseph Monier, 92859 Rueil-Malmaison, France
| Email : info@kaspersky.fr